White Paper

A Proposal for Protection of Unencrypted Digital Broadcast Television

December 6, 2002

1 Summary of Conclusions

1.1 The DTV transition promises new opportunities, but also poses new risks. The proposed implementation of the broadcast flag technology (the "Broadcast Flag Solution" or the "Solution") set forth in the accompanying documents is a practical, economical solution to the problem of piracy of digital broadcast television content, one that is necessary in order to protect digital broadcast television content and facilitate a meaningful DTV transition, allowing its promise to be fulfilled.

1.2 The Broadcast Flag Solution is limited in scope: it is designed to prevent unauthorized redistribution only of digital broadcast television content outside the personal digital network environment, as defined below. The Solution does not prevent or limit the number of physical copies from being made within the home. It requires only that such copies be sufficiently secure so as to prevent such copies from being a source of unauthorized redistribution outside the home.

1.3 The Solution is narrowly tailored to apply directly only to products containing certain devices called "demodulators," or other devices known as "modulators." Other products would be required to protect digital broadcast content only in two very limited circumstances, and only if their manufacturers elected to receive such content. Furthermore, the Broadcast Flag Solution preserves manufacturer flexibility to the greatest extent possible. Manufacturers that choose to participate would have a wide range of expanding options of protection technologies to choose from in designing their products. The Solution also promotes the interests of consumers who wish to receive high-quality digital television content. And the Solution provides a fair, market-based procedure, administered by the FCC, for determining protection technologies authorized for use in regulated products ("Table A technologies") that balances the interests of both content providers and manufacturers. Under this procedure, technologies may be authorized for use in protecting digital outputs or recording if it can be shown that they are already used or approved by content owners for the protection of valuable content, or if they are at least as effective as a technology that has already been authorized.

1.4 The outlines of the Broadcast Flag Solution have already received widespread, cross-industry support. This more specific proposal is put forward by the Motion Picture Association of America, Inc. ("MPAA"), ABC, ABC Television Affiliates Association, AFMA, American Association of Advertising Agencies ("AAAA"), American Federation of Television and Radio Artists ("AFTRA"), American Society of Composers, Authors and Publishers ("ASCAP"), Association for Maximum Service Television, Inc. ("MSTV"), Association of National Advertisers, Inc. ("ANA"), Belo Corp., Broadcast Music, Inc. ("BMI"), CBS, Directors Guild of America ("DGA"), Fox Broadcasting Company ("FBC"), International Alliance of Theatrical and Stage Employes, Motion Picture Technicians, Artists and Allied Crafts of the United States, its Territories and Canada, AFL-CIO, CLC ("IATSE"), National Association of Broadcasters ("NAB"), Screen Actors Guild, Inc. ("SAG"), Writers Guild of America, East, Inc. ("WGA-East"), and Writers Guild of America, West, Inc. ("WGA-West"). In addition, the proposal is also supported by the Digital Transmission Licensing Adminstrator, LLC (commonly known as "5C").

2 The Need for the Broadcast Flag Solution

2.1 Unlike other digital programming distribution methods such as cable, satellite, or DVDs, digital broadcast television is transmitted in the clear, and thus is subject to an extraordinarily high risk of unauthorized redistribution. Once received in the home, digital broadcast television content can easily be redistributed via retransmission over networks like the Internet by such means as rebroadcasting, hosting files on a web server, or peer-to-peer file trafficking. Such unauthorized redistribution can be accomplished without downloading any special software, without the need for circumventing any copy protections, without such tools as analog-to-digital converters, or indeed without any complex technical skills whatsoever. For example, all a person has to do is to select "Record" while watching TV on his or her computer using a TV tuner card, and then save the file to a publicly accessible folder on his or her hard drive, where it can be illegally redistributed to anonymous users via peer-to-peer file trafficking. Or that person can easily e-mail the file as an attachment to an unlimited number of people. Or he or she can simply place the recorded file on a personal webpage for unauthorized redistribution to others on the Internet. The capability of the Internet to allow distribution worldwide, instantly, to millions of recipients, distinguishes the looming threat of digital piracy from previous technologies, such as the VCR, that rely on the creation and distribution of physical copies. With worldwide unauthorized redistribution of digital content so easy to accomplish, the threat of widespread piracy is enormous, even if the number of pirates is low. Any recipient of digital broadcast television, not just the professional pirate or amateur hacker, would have it within his or her power to illegally redistribute digital broadcast television content almost at will, everywhere on Earth.

2.2 Without a regulatory redistribution control regime such as the Broadcast Flag Solution, content providers are faced with the spectre of digital piracy on a massive scale of whatever content they make available for digital broadcast. Given the extent of such piracy, it would be impossible to combat the unauthorized retransmission of digital content effectively merely by pursuing individual infringement actions. Rather, a comprehensive regulatory framework must be established to ensure the protection of digital broadcast content as it enters consumer products. Otherwise, as broadcast television transitions into the digital era and as broadband capacity expands, we can expect that producers of compelling programming will recalculate their interest in licensing their most valuable content over a distribution mechanism so easily susceptible to unauthorized redistribution, and will consider instead limiting such programming to more secure channels such as conditional access systems. The DTV transition may, as a result, be seriously threatened.

2.3 A regulatory redistribution control regime is also necessary to preserve free consumer access to high-quality programming by means of broadcast television. Broadcast television is a unique resource, justly cherished by millions of Americans. The availability of compelling programming free of charge via broadcast television has been a staple of American culture since the 1950s. In addition to its importance domestically, broadcast television programming is a major United States export that is tremendously important both to the American economy and to our prestige in the world. For all of these reasons, broadcast television is a critically important resource that must be preserved.

2.4 High-value broadcast programming exists only because of the market foundation on which it has been built. A multi-billion dollar industry, employing thousands of individuals, broadcast television depends on an economic model that relies not on fees collected from the individual consumer, but on advertising revenue and on profits from resale rights both here and abroad. Under this model, broadcast television content providers have invested millions of dollars in producing expensive, high-quality, high-production-value programming. This programming could not exist without the expectation of the revenue generated by sales of advertisements in particular geographic markets and by syndication of programs after their initial broadcast. Content owners, directors, writers, actors, distributors, and others all depend on the existence of that revenue stream for their compensation and their ability to produce and distribute new works. Broadcast television programming has also contributed to the enormously important consumer electronics and computer industries. The wide availability of high-quality programming has driven increasing demand for these products.

2.5 The viability of the economic model upon which the broadcast television industry is built will be seriously undermined by rampant piracy if digital broadcast television content is not protected. Unauthorized redistribution would inflict enormous damage on both of the pillars upon which broadcast television now stands. It would cripple advertising revenue by hindering broadcast content providers' ability to distribute content on a territorial basis and to adapt advertising to particular markets; and it would seriously damage critically important resale and syndication rights.

2.6 The result could be the destruction of broadcast television programming as we currently know it. The loss of valuable programming via free, over-the-air broadcast television would reduce the rich range of options consumers presently have in choosing the means of viewing valuable content. Indeed, poorer consumers who may not be able to afford conditional access subscription fees may be shut out of obtaining quality television programming entirely, a consequence that would exacerbate fears of the emergence of a "two-tiered" information society.

3 Overview of the Broadcast Flag Solution

3.1 Scope of the Broadcast Flag Solution

3.1.1 The Broadcast Flag Solution is designed to prevent unauthorized redistribution outside of the personal digital network environment. "Personal digital network environment" means the home or similar local environment. The "home" consists of all the rooms or areas within a consumer's primary residence. "Similar local environment" expands beyond the limited definition of "home" to include locations such as a consumer's car, boat, RV, or second home. "Personal digital network environment" thus covers any of these types of locations, but does not cover unauthorized or insecure transmission between or among them. That is, the Broadcast Flag Solution allows for a flexible definition of "personal digital network environment" to include electronic transmission of digital broadcast content between various locations typically associated with a consumer's home, but quite reasonably does not require content owners to accept unauthorized transmissions or intolerably low levels of security. Nor does the Broadcast Flag Solution itself limit a consumer's ability to make or move physical copies of broadcast content.

3.1.2 With respect to security, technologies to securely bind content to the personal digital network as it is being transferred between or among locations do not exist today. We invite and encourage the development of such technologies that could expand consumer choice so long as valuable rights in content are protected.

3.1.3 The Broadcast Flag Solution is not a form of broadcast copy protection. The Broadcast Flag Solution does not place restrictions on analog copying; for example, the Solution will have no impact on the use of VCRs. With respect to digital copying, the Solution allows the creation of digital recordings using authorized recording methods, and allows transmission between products using authorized digital outputs. Indeed, the technologies that MPAA member companies have thus far recognized as satisfying the criteria for Table A technologies — DTCP, HDCP, CPRM, and D-VHS — all allow secure digital transmission and recording within the personal digital network environment. We expect that future technologies will also satisfy the criteria in a similar manner.

3.2 Structure of the Broadcast Flag Solution

3.2.1 The Broadcast Flag Solution begins when a digital broadcast television signal is demodulated -- that is, converted from a radio waveform to a digital data stream. Demodulation is where the risk of unauthorized redistribution commences; prior to demodulation, the digital broadcast television signal is in an unusable, modulated form. It is therefore critical that the content be required to be protected from the point of demodulation forward. The Broadcast Flag Solution achieves this by regulating all consumer products containing demodulators, requiring such products to handle digital broadcast content in a secure manner until it has been checked for the presence of the Broadcast Flag, and to pass the content only to certain other products that will handle it securely until it has been checked for the Flag.

3.2.2 In order for the Broadcast Flag Solution to be complete, products receiving a digital signal from a product containing a demodulation device must also protect against unauthorized redistribution. However, such products would become subject to the Requirements only in the case where their manufacturers opt, by making a written commitment to follow the Requirements, to make their products eligible in two limited situations to access digital broadcast television content in usable form.

3.2.3 The vast majority of products will be designed either not to access digital broadcast television content at all in usable form, or to access such content only after it has been passed from a regulated product via a protected output. Such products are not subject to the Requirements, although the latter products would be subject to any licensing terms imposed by the manufacturer of a Table A technology used to pass the content. In the case of a product receiving content over an analog output, or over a restricted DVI output, no requirements are imposed.

3.2.4 Consumer modulators are also regulated under the Solution. A "consumer modulator" is a device that converts a signal into the same form as is used by a digital broadcast television station. Such modulators can be used as a means of connecting products to a home network. However, if unregulated, consumer modulators could also be used to mislabel content that

originated in another protected distribution channel, such as view-only content distributed over a broadband connection or encrypted pay-per-view transmissions, as copyable digital television content. In other words, left unregulated, consumer modulators could be used as a "laundry channel." In order to prevent such "Modulator Laundry Channels" from undermining other content protection systems, consumer modulators are required to refuse to pass content marked with the Broadcast Flag from "non-trusted sources."

3.3 Description of the Broadcast Flag Solution

3.3.1 Under the Broadcast Flag Solution, certain content may be embedded with the Broadcast Flag – the Redistribution Control descriptor set forth in ATSC Standard A/65A: Program and System Information Protocol for Terrestrial Broadcast and Cable, 31 May 2000, Amendment 3, 6 February 2002. The presence of the Flag means only that redistribution control is being asserted.

3.3.2 All consumer products containing demodulators, as well as certain other consumer products described above, must either check for the Flag, or protect the content as if it were marked with the Flag. If the Flag is found to be present, or if the content has not yet been screened, the product must protect the content from unauthorized redistribution under the Compliance and Robustness Requirements described below. If the Flag is not found to be present, the Requirements no longer apply.

3.3.3 Products specifically intended for professional and broadcast use are exempt from the Requirements. Retransmitters of DTV content in encrypted or unencrypted form, however, have additional obligations to ensure the protection of the content after retransmission.

4 Cost and Impact of the Broadcast Flag Solution

4.1 Of the available alternatives, the Broadcast Flag Solution accomplishes the protection of digital broadcast content in the most economical and practical manner. Implementation of the Broadcast Flag Solution will bring digital television into an already existing framework of content protection. The Broadcast Flag itself is royalty free, and the Broadcast Flag Solution is easily implemented and an efficient solution for both the product manufacturer and the consumer.

4.2 The Broadcast Flag itself is merely a message in the ATSC stream that is fully compatible with current ATSC-compliant devices. The Broadcast Flag Solution will not prevent consumers' existing equipment from displaying or recording content marked with the Flag. Since analog outputs are a permitted output under the Requirements, existing analog displays, players, and recorders will continue to function with the new compliant products under the Compliance and Robustness Requirements. Furthermore, the restrictions imposed by the Broadcast Flag Solution on digital outputs will hardly be unusual considering existing private contractual agreements for the protection of conditional access television and other forms of content. Enactment of the Broadcast Flag Solution will ensure that digital broadcast television is protected in a similar fashion as with every other form of digital audiovisual content, but without the limitations on copying that other protection arrangements may impose. Moreover, secure

copies will be viewable on the playback facility of the recorder that made them. Thus, any incidental incompatibility between secure recordings and legacy players will commonly involve distribution of the recording to other persons or locations. In order to achieve a balanced solution, however, this incidental legacy issue must not be used to undermine needed security of freely permitted copies.

4.3 As noted, the Broadcast Flag will in no way retard the development of new consumer technologies. Under the criteria for Table A, any technology that has achieved marketplace acceptance, or that is at least as effective as a technology already on Table A, can be added to Table as an authorized technology. We envision that Table A will grow to include a diverse population of authorized technologies as competing technology manufacturers vie to capture more market share. Four such technologies have already gained sufficient industry acceptance to qualify as authorized technologies, while several others are in development that have the potential to be equally effective.

4.4 Similarly, the Broadcast Flag Solution will not, in itself, interfere in any way with continued innovation in the development of open source software. While building a secure open source protection technology will no doubt be a challenge, it is a challenge faced by open source programmers in developing *any* secure application, not just Table A technologies. We welcome the efforts of open source programmers to meet this challenge and develop secure digital output protection technologies and recording methods for submission for inclusion on Table A.

4.5 The cost impact on affected products of implementing the Broadcast Flag Solution will be insignificant. Already, several technologies worthy of listing on Table A exist in the marketplace, even without the Broadcast Flag Solution, thus proving that such technologies are both affordable and readily available. The vast majority of products will also record, process, and display pay television and other types of content that will require such technologies be implemented even without the Broadcast Flag Solution. In addition, many products are already manufactured under private licensing arrangements that are very similar to the Compliance and Robustness Requirements. The existence of such products is additional proof that the cost impact of the Broadcast Flag Solution will be negligible.

5 The Compliance and Robustness Requirements

5.1 The Compliance and Robustness Requirements are the heart of the Broadcast Flag Solution. Together, these Requirements ensure both that digital broadcast television content is protected within regulated products, and that it cannot be transferred to a location that is insecure.

5.2 The Compliance Requirements restrict the types of outputs and recording methods that may be employed by regulated products. Under the Compliance Requirements, digital outputs and recording methods must be protected by one or more authorized technologies to prevent unauthorized redistribution. In limited cases, digital outputs and recording methods may be protected by a self-certified Robust Method, where the content has been neither screened nor processed after demodulation or where the content is passed in a certain way within a computer.

5.3 The Robustness Requirements require products to be secure against attempts to access protected content. The Robustness Requirements include the requirement, included in similar content protection technology agreements, that source products and Downstream Products "shall be manufactured in a manner clearly designed to effectively frustrate" attempts to modify such products to defeat the Compliance Requirements. Under the Robustness Requirements, products must meet a specified level of secure design and construction, for example, by employing encryption techniques and being tamper-resistant.

5.4 An additional requirement is necessary in order to prevent another form of the "laundry channel" problem – what might be called the Unscreened Content Laundry Channel. Under the Requirements, a product containing a demodulation device may output or record digital broadcast television content without screening the content first. Such "Unscreened Content" must be treated as if it contains the Flag, until it is screened. However, while the Requirements define "Unscreened Content" as digital broadcast television content, which is copyable, a product receiving such "Unscreened Content" has no way of determining whether the content is copyable broadcast television content or "Copy Never" content taken from elsewhere until the content is examined. If unexamined content is allowed to leave a compliant product via a Table A technology with no obligations to check for the Flag, such products could be used to mislabel content that originated in another protected distribution channel, such as view-only content distributed over a broadband connection or encrypted pay-per-view transmissions, as copyable digital television content. In order to prevent the creation of such an "Unscreened Content Laundry Channel," the Requirements provide that Table A technologies must check for the Flag, or require other products to do so.

6 Authorized Output and Recording Protection Technologies

6.1 One of the key components of the Broadcast Flag Solution is the provision that consumer electronics and computer manufacturers in most instances be required to use one or more of the Table A technologies in designing the digital outputs and recording methods of their products. Without such a requirement, there would be no guidance to product manufacturers as to what technologies to include, insufficient certainty concerning the standards to be met, and unavoidable contention between content providers and manufacturers concerning the meaning of the Requirements. Such an environment would be antithetical to the DTV transition, and would necessarily involve the FCC in constant adjudicatory actions.

6.2 The solution to this problem is to specify particular authorized output and recording protection technologies that regulated products may use. Instead of locking in technological mandates that may quickly become obsolete, or abstract concepts that offer little guidance, the Solution adopts a flexible, market-based approach under which a technology is authorized for Table A if it has been accepted in the relevant marketplace as a protection technology or is just as effective as one that has. The Broadcast Flag Solution contains fair and carefully balanced procedures for continually adding new technologies to the list. This method of protecting outputs and recordings ensures that innovation in the product manufacturing industry continues unabated. Continued innovation not only benefits technology manufacturers and consumers, but also content providers, who will benefit most of all from the creation of a continually evolving list of state-of-the-art technologies for content protection.

6.3 The Broadcast Flag Solution includes several procedures to determine if a technology has been accepted in the marketplace. If a technology provider believes its technology meets one of the criteria, it may file an application stating the grounds for its belief. The companies named in the application as having "used or approved" the technology in the market would then be requested to respond; if the companies do not respond to the request, they will be deemed to have admitted the facts alleged in the application. Any remaining dispute would be fairly but swiftly resolved by Commission staff.

6.4 While appropriately respectful of marketplace decisions, the Broadcast Flag Solution also includes a safeguard provision under which Commission staff may determine that the marketplace has been unreasonably slow in adopting a proposed technology that is just as effective as a technology already on Table A. The safeguard provision is intended to address any concerns about the fairness of market-based criteria. Indeed, the procedures for this safeguard provision are more detailed than any other procedure contained in the Broadcast Flag Solution. Under the safeguard provision, the proponent of a new technology that is "at least as effective" as a technology already on Table A may apply to have it added to the list. The Commission will issue a public notice providing 60 days for comment on the request to place the technology on Table A. In reaching its decision, the Commission staff will consider not only the effectiveness of the proposed technology in protecting digital television content from unauthorized redistribution, but also any applicable license terms of the technology relating to security, enforcement, and updates.

6.5 Although the proposed regulations do not identify particular technologies that should be added to Table A upon enactment, it is important that the Commission act immediately upon issuing these regulations to simultaneously identify appropriate technologies to be admitted to Table A. Swift approval of an initial set of technologies is necessary to facilitate the digital television roll-out, to protect digital broadcast television content as soon as the regulations become effective, and to inform manufacturers of the technical means of implementing the Broadcast Flag Solution.

6.6 The Broadcast Flag Solution recognizes that some Table A technologies may be compromised. Therefore, to protect against inevitable hacks, the Solution includes a procedure by which a request can be made to remove a technology from Table A if it has been compromised. The Commission would make a timely determination as to whether or not such technology should be removed from Table A. In doing so, the Commission would consider two factors: the protection of digital television against unauthorized redistribution, and the impact on content owners, consumers and manufacturers resulting from the continued use of the compromised technology and from any removal of the technology from the list.

7 Digital Broadcast Television Retransmitted by Cable and Satellite Systems

7.1 The Requirements apply only to "Unencrypted Digital Terrestrial Broadcast Content" -- content broadcast "without encrypting or otherwise making the content available through a technical means of conditional access." However, digital broadcast content should also be protected when retransmitted by cable or satellite systems. In the case of unencrypted cable

retransmission, the Requirements take hold upon demodulation by the consumer's set-top box, the same as DTV demodulation. Other retransmitters, however, such as direct broadcast satellite systems, not only use a variety of changing modulation methods not readily specified in the Requirements, but also encrypt retransmitted broadcast television signals, making it impossible to check such signals for the Flag until they are decrypted. In order to ensure that retransmitted digital broadcast television content is protected, the Requirements provide that retransmitters that encrypt digital broadcast television signals must either check for the Flag themselves at the head end or require the set-top box to check for the Flag on decryption of the signal. If the Flag is present, the retransmitter must require the consumer set-top box or other receiving productto abide by the Requirements as if it contained a covered demodulation function.

8 Effective Date

8.1 Consistent with industry practice, some period of time must be given before manufacturers must cease manufacturing and distributing products that are not in compliance with the Compliance and Robustness Requirements. Given the low cost and the technical ease of implementing the Broadcast Flag Solution, and the fact that no licenses will need to be negotiated to use the Flag, twelve months is a sufficient amount of lead time following adoption of the Requirements by the Commission.

[END]

A Quick-Reference List of Common Terms, Organizations and Standards for Digital Rights Management

G.E. Lyon
Convergent Information Systems Division
National Institute of Standards and Technology
Gaithersburg MD 20899-8951

The field of digital rights management (*DRM*), sometimes called intellectual property management and protection (*IPMP*), is today a chaotic and not always workable mix of technology, policy, law and business practice.[1] Under such circumstances, even a modest guide or index of major terms can be useful. In March 2002, a NIST cross-industry DRM workshop recommended that NIST take first steps toward such a guide. With the help of numerous workshop participants and others, this is the first edition of a DRM quick-reference list.

List Entries. Entries in the table constitute an attempt to assemble a *short set of descriptions*. The left side of each entry is a descriptor. The entry right side—somewhat *ad hoc* in layout—supplements by helping a reader explore further, usually on the World Wide Web[2]. Comments on earlier drafts indicate this format strikes an appealing balance for many readers. Entries convey some information, yet overall the list does not span too many pages. However, to succeed in depth, each entry relies heavily upon its indicated Web sites, which the reader must view to get fuller details.

Quick-Reference List of Common DRM Terms, Organizations and Standards

3GPP and 3GPP2 Third generation wireless systems transmit broadband, packet-based text, digitized voice, video, and multimedia at rates *circa* two megabits per second. The *Third Generation Partnership Project* is a collaboration and harmonization effort among telecommunications standards bodies; the current set has ARIB, CWTS, ETSI, T1, TTA, and TTC. Project 2 (*3GPP2*) does not include ETSI.	**DRM standards, coordinations, interests:** Major alliances: Cf. www.3gpp.org/Management/OP.htm Observers— ACIF, TIA, TSACC Liaisons—Wireless Multimedia Forum (WMF) **Membership:** Telecommunication standards bodies may be Organizational or Observer Partners. Other statuses described at www.3gpp.org/membership/membership.htm. **See:** www.3gpp.org and also www.3gpp2.org **Remarks:** 3GPP's TSG-SA (WG4) is responsible for Technical Specifications for Service and Applications, with WG4 concerned with DRM issues as related to wireless services.
4C Entity *4C Entity* licenses three DRM technologies—Content Protection for Prerecorded Media (CPPM), Content Protection for Recordable Media (CPRM), and the C2 Encryption Technology.	**Major alliances:** Cf. *CPTWG* entry. **See:** http://www.4centity.com **Remarks:** Currently, CPPM covers prerecorded DVD Audio and CPRM applies to recordable, removable media (DVD-R, -RW, -RAM, + two flash memory cards). 4C Entity offers C2 Encryption Technology, used for both CPPM and CPRM, independently for content on various media, removable or non-removable. The website also has information on the Content Protection System Architecture (CPSA) and on watermark application. CPSA is a conceptual framework for the integration of otherwise-independent content protection technologies (including CPPM and CPRM).
5C	Cf. *DTLA* entry.

[1] The list entry "DRM" briefly sketches some of the property management and protection roles.

[2] Special thanks go to F. Attaway, M. Baugher, B. Gandee, C. Garza, T. Hardjona, M. Hogan, V. McCrary, P. Schneck, J. Thurston and B. Turnbull for inputs, suggestions and corrections to earlier drafts.

AAP The *Association of American Publishers, Inc.* has developed standard requirements for publishers in the field of electronic books (e-books) and metadata for the electronic marketing of conventional books.	**DRM standards, coordinations, interests:** Major alliances: • EDItEUR (which see) • BISG (*Book Industry Study Group*, which see) Efforts developed with participation from the publishing and e-commerce industries. Has 310 company members. **Membership:** A system of regular, associate and affiliate tiers with dues based upon sales in the field of publishing. U.S. Companies are specified. **See:** http://www.publishers.org/, and especially Digital Rights Management for Ebooks: Publisher Requirements, available at www.publishers.org/home/drm.pdf **Remarks:** Defined requirements are voluntary and open standards.
ATSC The *Advanced Television Systems Committee*, Inc. is an international, non-profit membership organization developing voluntary standards for the entire spectrum of advanced television systems. Specific ATSC focusing is upon digital television, interactive systems, and broadband multimedia communications. ATSC has defined the digital TV standard for the U.S.	**DRM standards, coordinations, interests:** Major alliances: Key organizations contributing to the development of digital television and to the ATSC DTV Standard include the U.S. Congress and FCC, the FCC's Advisory Committee, the Digital HDTV Grand Alliance, and the ITU-R. Other liaisons— **Membership:** www.atsc.org/membership.html gives details. Open to corporations, non-profits and government on a sliding membership fees scale. **See:** www.atsc.org **Remarks:** DVB is the European equivalent undertaking (see below).
BASIC *Book And Serial Industry Communications* is a standards forum of BISG (see below). BASIC develops and maintains technology and electronic commerce standards.	**See:** www.bisg.org/basic.htm **Remarks:** Facilitates administration of electronic data interchange (EDI) formats for books and serials. Uses international EDI standards coordinated by EDItEUR, the international organization coordinating book and serial electronic commerce.
BIC The UK-based *Book Industry Communication* develops standards for e-commerce and communication in the book industry. BIC has three major focuses: bibliographic and EDI standards, the supply chain, and digital publishing.	**DRM standards, coordinations, interests:** Major alliances: EDItEUR, BISG **Sponsors:** The Publishers Assoc., The Booksellers Assoc., The Library Assoc., and the British Library. **See:** www.bic.org.uk **Remarks: See ONIX entry.**
BISG The *Book Industry Study Group* is spearheading the management of the On-Line Information Exchange (ONIX) and promoting the standardization of e-content and ONIX tagging for the better dissemination of electronic matter.	**DRM standards, coordinations, interests:** Major alliances: AAP, EDItEUR, BIC Other liaisons— **Membership:** Five tiers, with fees ranging from $500 to $6000 per year: university, non-profit, library, associate and commercial. **See:** www.bisg.org **Remarks: See ONIX entry.**
BPDG Broadcast Protection Discussion Group, a sub-group of CPTWG.	**Cf.** CPTWG entry. **Remarks:** Trying to resolve copy protection issue on DTV.
CDN	**A term signifying** *Content Distribution Network.* May designate an electronic infrastructure for materials (including streams) that have digital rights or intellectual property management (DRM/IPM) requirements. CDN issues include security, efficient storage including caching, availability and quality of service.

CEN/ISSS *Comité Européen de Normalisation* develops European technical standards. Experts work through Technical Committees (TCs), of which eight—all IT related—are in the Information Society Standardization System. ISSS aims for rapid market-driven informal specification plus the security of conventional, formal, open standardization. New, special DRM project examines standardization of technologies for digital rights management.	**DRM standards, coordinations, interests:** Recent ISSS draft DRM report widely circulated, see europa.eu.int/information. In March 2002, began an inventory of DRM standards work on sector, status, membership, schedules, process, activity, outputs, etc. society/newsroom/documents/drm_workingdoc.pdf and also the URL www.cenorm.be/isss/Projects/DRM/NEW_WEB_SITE_Revised.htm **Membership:** The DRM Group is open to any CEN/ISSS Forum member entity, or their representative, and to additional interested parties. **See:** www.cenorm.be/isss/ **Contacts:** giulia.cipressi@cenorm.be, James.Boyd@cenorm.be **Remarks:** CEN/ISSS represents the European Union at the international level, e.g. ISO.
cIDF Like the DOI (below) , the *content ID Forum* develops specifications for content identification and metadata that enable e-commerce and rights transactions for copyrighted information. cIDF and DOI have agreed to collaborate on building an infrastructure for the management of digital intellectual property.	**DRM standards, coordinations, interests:** **Partners:** ISO/MPEG, Indecs, IDF (DOI), TV Anytime Forum, DCForum, AMF, MAA, DCAj, AMD, CG-Arts Assoc., ARIB **See:** www.cIDF.org **Remarks:** Established by Prof. H. Yasuda at the University of Tokyo. Provides mechanisms for copyright management, cooperates with other standardization bodies throughout the world.
CPTWG The *Copy Protection Technical Working Group* is an *ad hoc* public forum for discussing content protection technologies that inhibit access, use, or reproduction not authorized by copyright owners; CPTWG's meetings are attended by companies in the industries of content (esp. video and audio), consumer electronics, information technology, copy protection, and, by consumer interest groups.	**DRM standards, coordinations, interests:** **Formal:** The Broadcast Protection Discussion Group (BPDG) is a discussion group created by the CPTWG. **Interactions**—See http://www.cptwg.org/html/LINKSPAGE.htm; also see entries for DVD CCA/CSS, 4C, DVD Forum, HDCP, DVD+RW Alliance. **Membership:** Formed by CEA, MPAA and the Information Technology Industries Council (ITI), with further support from RIAA and BSA **See:** http://www.cptwg.org **Remarks:** Presentations are made by vendors and experts. Discussion groups form to provide more in-depth review of particular issues when that is desired by the participants. Meetings are public forums held at the Renaissance Hotel, 9620 Airport Blvd., Los Angeles, CA (at airport).
DOI (IDF) The International DOI Foundation states, "The Digital Object Identifier (DOI®) is a system for identifying and exchanging intellectual property in the digital environment. It provides a framework for managing intellectual content, for linking customers with content suppliers, for facilitating electronic commerce, and enabling automated copyright management for all types of media." The DOI is a "persistent identifier of intellectual property entities". Unlike a URL, it does not point to a location.	**DRM standards, coordinations, interests:** Major alliances • WIPO (World Intellectual Property Organization) • ISO (International Standards Organization) • NISO (National Information Standards Org.) • IETF (Internet Engineering Task Force) • W3C (World Wide Web consortium) • OEBF/EBX (Electronic Book Exchange) • MPEG-21 (ISO Multimedia Framework—see entry MPEG) Other liaisons— CENDI, CIDF,CNRI, EDItEUR, ICE, <indecs>, XBRL; *cf.* 8.0 of DOI Handbook at www.doi.org/handbook_2000 **Membership:** Open to those interested in electronic publishing and related technologies. Non-members welcome to contribute. **See:** www.doi.org **Remarks:** Work is evolving rapidly.

DCMI (Dublin Core) The *Dublin Core Metadata Initiative* is an open forum engaged in the development of interoperable online metadata standards that support a broad range of purposes and business models.	**DRM standards, coordinations, interests:** Major alliances—See www.dublincore.org/about/participants/ for details. National library systems, etc. Other liaisons— CEN, IEEE/LOM, IETF, MPEG, NISO, W3C, PRISM; see www.dublincore.org/about/liaisons/ **Membership:** Open—participate by joining the appropriate mailing list for the working group activity of interest. **See:** www.dublincore.org **Remarks:** Standardized in the IETF as RFC 2413
DMCA World Intellectual Property Organization (WIPO) treaties gave impetus to U.S. legislation called the *Digital Millennium Copyright Act* of 1998. To facilitate digital, e-commerce growth, Congress implemented legislation that addresses WIPO treaty obligations not adequately addressed under existing U.S. law.	**Origin:** U.S. Congress "...But as Congress recognized, the only thing that remains constant is change. The enactment of the DMCA was only the beginning of an ongoing evaluation by Congress on the relationship between technological change and U.S. copyright law. This Report of the Register of Copyrights was mandated in the DMCA to assist Congress in that continuing process...." *From* www.loc.gov/copyright/reports/studies/dmca/dmca_executive.html **Level of controversy:** Very high, both nationally and internationally
DTLA, (5C DTLA) The *Digital Transmission Licensing Administrator* handles matters on the use of the DTCP (digital transmission content protection) method, which is licensed. DTCP details are available through the DTLA via terms of a nondisclosure agreement.	**DRM standards, coordinations, interests:** Major alliances—5C=(Intel, Toshiba, Sony, Hitachi, Panasonic). Other liaisons—CPTWG (which see) **Membership:** **See:** http://www.dtcp.com/ **Remarks:** Content protection particularly aimed at transport on high performance digital buses.
DREL	Cf. *IEEE/LOM* remarks.
DRM *Digital Rights Management* is a system of information technology (IT) components and services, along with corresponding law, policies and business models, which strive to distribute and control intellectual property and its rights. Product authenticity, user charges, terms-of-use and expiration of rights are typical concerns of DRM.	For a generic DRM transaction, imagine A gets a request to send digital material X to B. The digital content X is typically combined by producer A with tracing information, giving (X + t). This tagged content is then encrypted along with rights-rules (RR) and user/document identifiers (ids) to yield *e*(X +t +RR + ids). A sends this result, *e*(...), to B. B has a compatible receiving environment, sometimes a special tamper-resistant reader, in which *e*(...) can be properly decrypted and used. The key to *e*(...) may be sent encrypted with B's public key if there is one; B (and only B) then uses its private key to decode the message key. A third-party clearinghouse H receives and sends payments, logs trace information and controls authorizations to A and B as appropriate.
DVB The *Digital Video Broadcast* project is an international industrial consortium of broadcasters, electronics manufacturers, network operators, software concerns and regulatory bodies. DVB is committed to designing European standards for the delivery of digital television and data services.	**DRM standards, coordinations, interests:** Major alliances: MPEG **Membership:** Cost = 10K euros ($9.2K) and member's activities should fit one category—broadcasters, network operators, regulatory bodies, manufacturers/developers, or, academic institution. **See:** http://www.dvb.org **Remarks:** Uses MPEG-2 packets as information payload containers. Supplies critical Service Information with packets. See ATSC for North American equivalent. CP and CPT—copy protection and CP(technical)—are DVB ad-hoc groups. Status of IPRM (the intellectual property rights module?) is unclear. ATSC (see entry) is North American equivalent effort.

DVD+RW Alliance This alliance comprises PC manufacturers, storage vendors and electronics manufacturers.	DRM standards, coordinations, interests: Major alliances Other liaisons—Cf. CPTWG Membership: http://www.dvdrw.com/join.html See: www.dvdrw.com Remarks: There is no membership fee or contract. Membership includes developing DVD+RW products within specific time windows (a year or so).
DVD Forum The *DVD Forum*—an international association of hardware manufacturers, software firms and other users of Digital Versatile Discs—exchanges and disseminations ideas and information about the DVD format. The Forum works to promote broad acceptance of DVD products on a worldwide basis, across entertainment, consumer electronics and IT industries.	**DRM standards, coordinations, interests:** Major alliances Other liaisons—CPTWG **Membership:** Open to corporations or organizations linked to DVD research, development or manufacturing, or software firms and other users of DVD products interested in improving the DVD Format. **See:** http://www.dvdforum.org/ **Remarks:** Promotes broad acceptance of DVD products worldwide, across entertainment, consumer electronics and IT industries. Membership exceeds 230 companies.
DVD CCA/CSS *DVD Copy Control Association* is a not-for-profit corporation with responsibility for licensing CSS (*Content Scramble System*) to manufacturers of DVD-related products.	**DRM standards, coordinations, interests:** **See:** www.dvdcca.org **Remarks:** See CPTWG, above.
EBNA "The *E-Book Newsstand Association* serves as the meeting place for companies active or interested in the delivery of periodical information to consumers or business customers via Electronic Books, Personal Digital Assistants, or Electronic Paper." *from Website*	**DRM standards, coordinations, interests:** Major alliances Other liaisons— **Membership:** Relatively inexpensive; open to companies and individuals. **See:** www.ebna.org **Remarks:** E-publishing is a representative class of users from DRM technologies and services.
EDItEUR *EDItEUR* is the pan-European book sector EDI Group. An British-incorporated company, it co-ordinates development, promotion and implementation of electronic commerce in the book and serials sectors.	**DRM standards, coordinations, interests:** Major alliances: Recognized by the Commission of the European Union and by the Western European EDIFACT Board; supported by the European Federations of Library, Booksellers and Publishers Associations Other liaisons— International, with 90 members from 17 countries **Membership:** Open to enterprises with interests in EDI for the book trade, and, to related associations **See:** http://www.editeur.org **Remarks:** See *ONIX*. Refer to www.editeur.org/ddd2_01.doc for the related EPICS data dictionary.
EPICS/ONIX *EPICS* refers to a comprehensive data dictionary developed by EDItEUR (see entry, above) and incorporated into the ONIX effort.	**Comment:** EDItEUR maintains the EPiCS/ONIX family of standards; the family addresses the electronic use of information on book products. Also, see *ONIX*.
HDCP *High-bandwidth Digital Content Protection* is a specification developed by Intel Corporation to protect digital entertainment content across the DVI interface.	**DRM coordinations, interests:** Confer entry for *CPTWG*. **See:** http://www.digital-cp.com/ **Remarks:** HDCP specification implementation requires a license.

ICE The *Information and Content Exchange* is a protocol and management model for information reuse among Web sites—syndication. It promotes automated data transfer and management of results.	**DRM standards, coordinations, interests:** Major alliances • PRISM—Syndication (e.g. between Web sites) requires a common vocabulary. PRISM can describe ICE items, and, ICE can convey PRISM descriptions. Other liaisons— W3C **Membership:** Open, modest yearly charge. 25% discount for Int. Digital Enterprise Alliance members. Authoring Group membership fee is 10x higher. **See:** www.icestandard.org www.w3.org/TR/NOTE-ice **Remarks:** Section 1.2 of note at www.w3.org/TR/NOTE-ice gives good number of details on relationships to other standards.
IDF International DOI Foundation.	**See:** Entry for "DOI."
IEEE/LOM The *IEEE* P1484.12 *Learning Object Metadata* Working Group specifies syntax and semantics of Learning Object Metadata—attributes that describe entities used during technology-supported learning.	**DRM standards, liaisons, interests:** Prometeus MoU: http://prometeus.org ; The IMS Project: http://www.imsproject.org; The Ariadne Project: http://ariadne.unil.ch ;European Schoolnet: http://www.en.eun.org ; IEEE/LTSC: http://grouper.ieee.org/groups/ltsc ; Virtual European School: http://www.ves.eu.org ; CEN/ISSS WS/MMI-DC ; ISO/IEC JTC1/SC36:http://www.jtc1sc36.org **Membership:** Open, dues $200/year. **See:** http://ltsc.ieee.org/wg12/s_p.html **Remarks:** Learning Objects include, *e.g.,* multimedia content, instructional materials, software and tools. Co-sponsors workshops Rights Expression Language (DREL), see www.cenorm on Digital.be/isss/Workshop/It/.
IETF The *Internet Engineering Task Force* has no specialized DRM group, but it does have group key management efforts such as GDOI (*Group Domain of Interpretation Rekey protocol*) and MIKEY (*Multimedia Internet KEYing*) within its MSEC Working Group.	**DRM standards, coordinations, interests:** Major alliances: W3C (Cf. *XKMS* entry) Other liaisons— IRTF (GSEC Working Group) **Membership:** Open to any interested individual w/out charge. **See:** www.ietf.org **Remarks:** Key management standards needed for DRM.
IFPI *IFPI* represents the international recording industry: It fights music piracy, promotes fair market access and adequate copyright laws. helps develop legal conditions and technologies for industry in this digital era, and promotes music as an economic factor in addition to its social and cultural contributions.	**DRM standards, coordinations, interests:** Major alliances: IFPI works with its 46 national groups through international and regional offices Other liaisons—Closely affiliated with the RIAA (www.riaa.org). **Membership:** Entity or person producing sound recordings or music videos available publicly in reasonable quantities. **See:** http://www.ifpi.org **Remarks:** A part of DRM involves interdiction, i.e., getting local authorities to enforce information protection laws against piracy. IFPI places heavy emphasis upon this aspect (see Web pages).

INDECS INDECS is an international initiative of rights owners creating metadata standards for e-commerce. <indecs>™ stands for interoperability of data in e-commerce systems—it stresses structured metadata and data dictionary for interoperability. <indecs>™ Framework Ltd is a not-for-profit company encouraging well-formed metadata initiatives based on <indecs> methods. The project is supported under European Commission info2000 that embraces multimedia rights clearance systems (MMRCS).	**DRM standards, coordinations, interests:** Major alliances ALCS (Authors' Licensing and Collecting Society Limited) www.alcs.co.uk MCOS (UK, musical works, Composer/publisher societies) BILD-KUNST (Germany, visual arts, creator's society) SACD (France, audiovisual and visual arts, creator's society) IFPI (International/UK-based, sound recordings, trade association) EDItEUR (European/UK-based, book/serial/electronic publishers/libraries) KOPIOSTO (Finland) (Co-ordinating Partner) CEDAR (Netherlands) CAL (Australia) MUZE UK (UK subsidiary with MUZE US parent) Other liaisons— Many. See http://www.indecs.org/project/affiliates.htm **Membership:** Partnership (cf. *alliances*, above) **See:** www.indecs.org **Remarks:** Affiliates include US Copyright Office, RIAA
INDECS2 <indecs2> is a follow-on project to create a rights data dictionary (RDD) spurred by requirements of MPEG-21 for a "consistent, ordered and machine-readable set of semantics ... describing the rights in intellectual property ... for permissions, such as 'print', 'copy', or 'play', to be reliably and securely controlled for all information in digital form, online and offline."	**DRM standards, coordinations, interests:** Major alliances—EDItEUR/ONIX, Int. DOI Foundation, RIAA/IFPI, MPA, Accenture, XrML (ContentGuard), Dentsu, Enpia are consortium partners. Other liaisons—XML, WIPO, MPEG(21) **Membership:** Partners **See:** **Remarks:** Responding to MPEG call using ISO/MPEG process; DOI dictionary as input; DOI developments will use output.
IPTC--NewsML The International Press Telecommuni-cations Council has two specifications for news (see NITF, below). NewsML supports automated *transmission* of news stories and wire services. It is an XML-based standard to represent and manage *multi-media* news throughout its lifecycle, including production, interchange, and consumer use.	**DRM standards, coordinations, interests:** Major alliances • with PRISM on common format and metadata vocabulary • XML Other liaisons—Use appropriate standards and recommendations. **Membership:** An independent international association of the world's leading news agencies and publishers. **See:** www.newsml.org **Remarks:** PRISM, NewsML "largely complementary." PRISM vocabularies can be used in NewsML. To replace IIM. Extensible and flexible. Use NITF for text with NEWSML. Plug-in NewsML parser available for browsers.
IPTC--NITF The IPTC also has an XML DTD (grammar) specification for news mark up. Called NITF for *News Industry Text Format*, it uses the eXtensible Markup Language (XML) to *define the content* and structure of news articles. With embedded metadata, NITF documents are far more searchable and useful than HTML pages.	**DRM standards, coordinations, interests:** Major alliances • work with PRISM Other liaisons— **Membership:** An independent international association of the world's leading news agencies and publishers. **See:** www.nitf.org/ **Remarks:** PRISM group says "largely" complements their specification. NITF documents translate into HTML, WML (wireless devices), RTF (for printing), etc. State "it is a standard that is open, public, proven, well-used, well-documented, and well-supported."

IRTF/IDRM *Internet Research Task Force/Internet Digital Rights Management* group examines new information rights technologies that impact the Internet. Seeks intellectual property network protocols and mechanisms that interoperate. Examples: directories, trust, privacy, policy, transport and security services.	**DRM standards, coordinations, interests:** DOI; <indecs>; MPEG/MPEG4 IPMP (mpeg.telecomitalialab.com/standards/ipmp/index.htm); W3C DRM 2001 Workshop www.w3.org/2000/12/drm-ws/; SDMI; XrML; ISMA; ODRL; XACML OASIS; MSEC/(GDOI and MIKEY) IETF working group covers key dissemination needed for DRM www.securemulticast.org/mscc-meetings.htm. **Membership:** open **See:** http://www.idrm.org/ for informative Web site **Remarks:** IRTF research complements engineering of IETF. Coordinates with IETF, other IRTF groups, to spot missing technology, recommend technical standards, etc. Note: Group charter revision underway, name change likely from IDRM.
IRML	See remarks portion of *XBML*.
ISMA As standard XML based mark-up languages have fueled innovation and growth of today's Web, so strives the *Internet Streaming Media Alliance* to accomplish the same for the next wave of rich Internet content, streaming video and audio.	**DRM standards, coordinations, interests:** Major alliances: 35+ corporate entities have joined. Other liaisons— **Membership: See ism-alliance.tv/html/join/indexjoin.shtml for costs of joining.** **See:** ism-alliance.tv **Remarks:** The first specification from ISMA defines an implementation agreement for streaming MPEG-4 video and audio over IP networks. On-going work includes adopting methods for digital rights management (DRM), quality of service (QoS) and related technologies.
ITU-T The *International Telecommuni-cations Union* is an organization within the United Nations system.	**See:** www.itu.int/ **Remarks:** ITU-T recommendations developed by the Telecommunication Standardization Sector (formerly CCITT) constitute the basis for international telecommunication standards.
MIME *Multipurpose Internet Mail Extensions* specifies formatting for non-ASCII messages for transmission over the Internet. Graphics, audio, and video files via the Internet mail system. In addition, MIME supports messages in character sets other than ASCII.	**DRM standards, coordinations, interests:** Major alliances: Other liaisons— **Membership:** **See:** xxx.m **Remarks:** Defined in 1992 by the Internet Engineering Task Force (IETF—see *IRTF* "remarks"). The newer S/MIME, supports encrypted messages. Has types, e.g., GIF for graphics files and PostScript for formatted files. It is also possible to define your own MIME types

MPEG The *Moving Picture Experts Group* is an ISO/IEC working group for standards development of coded representation of digital audio and video. MPEG has a series of specifications promoting content interoperability pertinent to DRM: MPEG-2 A/V content for DVD and TV. MPEG-4 multimedia content representation (metadata). MPEG-4 IPMP (intellectual property management and protection) addresses connected appliances, with work on standalone progressing. MPEG-7 content description (complements MPEG-4) MPEG-21 sweeping, ambitious framework for interoperable digital multimedia, transparent in use, user-friendly in practice.	**DRM standards, coordinations, interests:** • ISMA (Internet Streaming Media Alliance) uses MPEG-4 • ITU-T/MPEG video coding work for MPEG-4 • IRTF/IDRM • W3C is interested in MPEG work, but thus far (5/02) reticent to pursue DRM. • XML, e.g., in MPEG-21 Digital Item Description--DID, also ODRL (XML-based digital rights language) submitted to MPEG-21 responding to Call for Requirements. • Annex C (pp. 38-45) of report ISO/IEC 21000-1 points to many places of possible collaboration: www.tele.ntnu.no/users/andrew/Papers/MPEG-21-Part-1.pdf **Membership:** Requires accreditation by a National Standards Body or standards committee in liaison. Experts attending MPEG not representing a committee in liaison must be members of a National Delegation under the responsibility of a Head of Delegation appointed by the National Body. **See:** http://mpeg.telecomitalialab.com/ **Remarks:** Note that *DRM = IPMP* in MPEG parlance.
MMS 3GPP has defined a *Multimedia Messaging Service* that supports mobile user transactions via messages containing multimedia elements.	**See:** 3GPP entry, above. **Remarks:** MMS builds on SMS (Short Message Service). It makes Internet/mobile phone messaging much richer, exchanging text, graphics, audio, photographic images and video clips between mobile devices. MMS is not, however, real-time.
NewsML, *News Markup Language*	**See** XBRL entry, "Remarks."
OASIS XACML The OASIS *eXtensible Access Control Markup Language*, XACML, is an XML specification for expressing policies for information access over the Internet. Issues to be addressed include fine grained control, requestor characteristics, protocols over which requests are made, and types of activities authorized.	**DRM standards, coordinations, interests:** Major alliances: W3C, IETF, UN/CEFACT Other liaisons—Several efforts involving XML and electronic security are deemed germane to XACML and have liaisons to help ensure interoperability and to avoid duplication of work: - ebXML—e-business application of XML , - XKMS—distribution/registration of public keys, - DSML— directory information in XML **Membership: Open in three levels of participation:** sponsor, contributor, and individual. Details at www.oasis-open.org/join/ **See:** www.oasis-open.org/ **Remarks:** XACML defines a core schema and corresponding namespace for the expression of authorization policies in XML against objects that are themselves identified in XML.
ODRL The *Open Digital Rights Language* provides semantics for a digital rights management expression language and data dictionary. ODRL pertains to digital content in all forms: it expresses terms and conditions—permissions, constraints, obligations, conditions, offers and agreements with rights holders. ODRL is designed for extension by different industry sectors (eg ebooks, audio, software) while retaining a core inter-operability. ODRL is freely available: There are no licensing requirements.	**DRM standards, coordinations, interests:** Major alliances • **ODRL** supports MPEG-21. It will be a compatible Rights Language supporting open and free interoperability within and across the MPEG-21 Multimedia Framework. • **HTML and XML bases** Other liaisons— Has commercial and academic supporters. **Membership:** **See:** odrl.net **Remarks:** See XrML.

OeBF (including EBX) *Open eBook Forum,* an international trade and standards group, welcomes hardware and software companies, publishers, authors, users of electronic books, and related organizations. OeBF provides a forum for the discussing issues and technologies related to electronic books, and, for developing and promoting adoption of common specifications and interoperable standards relating to electronic books.	**DRM standards, coordinations, interests:** Major alliances • BISG (Book Industry Study Group www.bisg.org) • DOI (Digital Object Identifier www.doi.org) • W3C (World Wide Web Consortium www.w3.org) • NISO (National Information Standards Org. www.niso.org) • The Daisy Consortium (www.daisy.org) Other liaisons—AAP, Amer. Fed. Blind **Membership:** Principal Member subscribers have major voting rights. Corporations, organizations and private individuals may also join at nominal cost as non-voting Associate Members, who may, when approved by Working Group chairs, become voting members of Working Groups. **See:** www.openebook.org = www.ebxwg.org **Remarks:** EBX is now part of the OpenEBook Forum
ONIX International The *Online Information eXchange* is a standard format used to distribute information about books electronically. The rich ONIX metadata (may have audio or video) replaces the information on the jacket cover. ONIX is a standard format for easy, automated use in the Web-supported supply chain by a variety of book wholesalers, retailers, and others.	**DRM standards, coordinations, interests:** Major alliances: AAP, EDItEUR, BISG, BIC Other liaisons: BASIC (Book And Serials Ind. Communications) **Membership:** Typical committee members include American Booksellers Assoc., AAP, AAUP, AWBA, Amazon, Barnes & Noble **See:** www.editeur.org (Europe), www.bisg.org (US), www.bic.org.uk (UK) **Remarks:** Future issues include provision for e-books, videos and for DRM elements. Based on the ubiquitous XML with an ONIX DTD (document type definition). Major on-line booksellers use it.
PRISM *Publishing Requirements for Industry Standard Metadata* specification—is an extensible XML metadata standard for syndicating, aggregating, and generally, multi-targeting content for the printed medium. It supports interoperable content description, interchange, and reuse. Applications can be implemented without fees, but they must not modify PRISM namespaces and vocabularies. Unlike XrML, assumes in-place business arrangement. Aims at inexpensive use.	**DRM standards, coordinations, interests:** Major alliances • IPTC-NEWSML complements and overlaps PRISM; groups coordinate • PRISM recommends XML, RDF, the Dublin Core, and various ISO specifications for locations, languages, and date/time formats. • Beyond the above, it defines a small number of XML namespaces and controlled vocabularies of values. **See:** http://www.prismstandard.org/techdev/prismspec1.asp **Remarks:** A simplified application of RDF, but compatible. Uses Dublin Core vocabulary. Complements ICE. Complements, overlaps NITF from IPTC. Can use MIME for metadata packaging. Refer to http://www.oasis-open.org/cover/prism.html.
RDF The W3C *Resource Description Framework* model uses XML to represent and transport metadata.	**See:** remarks in W3C entry **Remarks:** PRISM (cf. above) uses a simplified resource description framework, RDF.
RIXML	See remarks for entry *XBRL.*

SDMI The **Secure Digital Music Initiative** comprises roughly 150 participants representing a spectrum of information technology companies and allied music interests. SDMI's charter has been to develop open technology specifications that protect the playing, storing, and distributing of digital music so that a new market for digital music can emerge. SDMI has aimed at: • Providing convenient access to music online and via novel advent digital distribution • Assuring copyright protection for artistic works • Promoting development of new, music-related business and technology.	**DRM standards, coordinations, interests:** Major alliances—150 participants. Other liaisons— see Membership, below. **Membership:** Open to technology-based commercial companies having significant direct effect on digital music security. Societies and associations representing music industry interests who are members of the Music Industry Advisory Council may participate as observers. **See:** www.sdmi.org **Remarks:** SDMI has suffered a lack of sufficient technology to assure its requirements. Quoting text dated May 18, 2001, from the SDMI Website, "... SDMI is now on hiatus, and intends to re-assess technological advances at some later date. This decision does not affect the prior adoption of SDMI's portable device specification and Phase I watermark, which are in widespread use today."
SMPTE (DC28.4) The *Society of Motion Picture Engineers* has a Technical Committee on Digital Cinema (DC28). In particular, DC28.4 works on specifications for security and rights related to digital cinema.	**DRM standards, coordinations, interests:** Major alliances Other liaisons— **Membership:** **See:** http://www.smpte.org/ **Remarks:**
W3C The *World Wide Web Consortium's* Technology and Society Domain held a workshop on DRM in January, 2001. However, domain participants have been slow to join any DRM effort, many apparently content to have MPEG and others pursue the complex topic.	**DRM standards, coordinations, interests:** • W3C Workshop on Digital Rights Management for the Web (January 2001) http://www.w3.org/2000/12/drm-ws/ • Cooperation with MPEG highly likely if W3C does DRM work **See:** www.w3.org/TandS/Signature discusses IP rights as a future W3C/T&S topic. **Remarks:** W3C develops specifications, guidelines, software, and tools that support the World Wide Web: these include the Resource Description Framework—RDF—to represent and transport metadata (www.w3.org/RDF), HTML, and XML.
WAEA The *World Airline Entertainment Association* has a Technology Committee that includes a Digital Content Management Working Group. At a technical level, the association addresses hardware and content specifications for commercial aircraft.	**DRM standards, coordinations, interests:** Major alliances: airlines, studios, device manufacturers, digital materials labs, service providers. Other liaisons— ARINC, SMPTE, ISMA, MPEG-4 Forum **Membership: representatives from over 100 airlines and 300 airline suppliers and related companies. Membership fees vary from $350 to $700 per annum.** **See:** http://www.waea.org/ **Remarks: The WAEA has produced a number of open, voluntary standards for content on aircraft, including DVD (Specification 0598) and video-on-demand file servers (Specification 0395).**

WAP Forum Content Download The *Wireless Application Protocol Forum* Ltd. has begun addressing DRM-IPMP issues in *content download*, including authentication, delivery, rights management, logging and billing.	**Possible Effort Co-ordinations:** 3GPP, SDMI, ISO/MPEG/IPMP, ODRL, XrML, XMCL **Membership:** http://www.wapforum.org/who/join.htm Full WAP membership costs $35K. Associates pay $7.5K p.a. **See:** www.wapforum.org/who/ActivityProp/ContentDownloadActivityProposal.pdf for activity proposal. **Remarks:** Proposal dated 11 December, 2001.
WIPO The *World Intellectual Property Organization*, an agency of the United Nations, promotes the use and protection of intellectual property (IP). It administers 23 international treaties dealing with different aspects of IP protection. There are two IP categories: i. Industrial property—patents, trademarks, etc.. ii. Copyright—novels, poems, films, music, drawings, photographs, sculptures, architectural designs, etc.	**DRM standards, coordinations, interests:** Major alliances: 179 Member States Other liaisons—170 NGO Observers **Membership:** only States may qualify **See:** www.wipo.org **Remarks:** Budget is $434M p.a. Regarding DRM, the Web site states, "Under its Digital Agenda – a work program for the Organization over the coming years, WIPO is responding to the confluence of the Internet, digital technologies and the intellectual property system. The Organization is formulating, through international discussions and negotiations, appropriate responses that will encourage dissemination and use of intellectual property such as music, films, trade identifiers and knowledge on the Internet, as well as ensure protection of the rights of their creators and owners."
WMF The *Wireless Multimedia Forum* is an international, multi-vendor venue for those developing products, services and information for rich media content for mobile, wireless devices.	**Liaisons**—See entries for *3GPP2, ISMA* **Membership:** Approximately 35 hardware vendors, software makers, carriers and content developers. See: www.wmmforum.com (note: is commercial site) Remarks: The *Wireless Multimedia Forum* has an Application Requirements Working Group interested in market requirements for DRM services.
XACML	See entry *OASIS XACML*.
XBRL The *eXtensible Business Reporting Language* is an open specification that uses XML-based data tags to describe financial statements: XBRL encoded financial information works across automated supply chains.	**DRM standards, coordinations, interests:** The natural constituency is the financial community, but this crosses over into DRM territory. **See:** www.xbrl.org, www.rixml.org, www.irml.org **Remarks:** XBRL can be seen as a possible contribution to the reporting and managing aspect of DRM related to finance. Other XML dialects may enter in as well, *e.g.* for investor research, there is RIXML and IRML (the latter stressing conversational use). NewsML, a news data markup specification, is similarly related.
XKMS The *XML Key Management Specification* defines protocols for distributing and registering public keys that are compatible with the XML Signature (XML-SIG) standard work of W3C and IETF and another anticipated standard for XML encryption.	**Support:** W3C, IETF are doing this Other liaisons— IRTF, OASIS (XML) **See:** www.w3.org/2001/XKMS/ **Remarks:** DRM will use encryption technology, especially that related to XML. See IETF entry.

XMCL The *eXtensible Media Commerce Language* is an open, XML variant for industry-wide standards in Internet (multi) media commerce. XMCL may simplify deployment and enlarge the market for digital media over the Internet.	**DRM standards:** XMCL Web site states: "RealNetworks intends to submit the XMCL proposal to the appropriate standards organization, and will work with other industry leaders to ensure the initiative evolves into a widely accepted standard." **Membership:** Abril Group, Accenture, Adobe Systems, Anystream, America Online, Artesia Technologies, Avid Technology, Bertelsmann, British Telecom's BTopenworld, Clear Channel, Context Media, EMI Recorded Music, eMotion, IBM, IFILM, InterTrust, MGM, Napster, RealNetworks, Rightsline, Sony Pictures Digital Entertainment, Starz Encore Group, Sun Microsystems, Tiscali, Viant, and Virage **See:** www.xmcl.org **Remarks:** XMCL standardizes the expression of business rules, and thus, enables content management independent of DRM (IPMP) and host e-commerce infrastructure.
XML The *eXtensible Markup Language* XML is actually a markup language to create other markup languages (and there have a lot of them thusly crafted). XML is extensible, license-free, platform-independent and well-supported. Its prolixity is usually redeemed by its wide acceptance and flexibility.	**DRM standards, coordinations, interests:** Widespread coordinations: E.g., go to www.xml.org and click on "XML in Industry." **Membership: NA** **See:** www.xml.org **Remarks:** XML is widely used in recent e-commerce designs because structured and labeled data is necessary for the flexible, open-ended automation of information services. Related entries are "X-series" XBRL, XMCL, etc. (see pointers by RIXML, IRML and NewsML).
XrML *EXtensible rights Markup Language*— XrML— is a XML-based vehicle for digital rights management. It aims at providing a universal method for specifying rights and conditions associated with the use and protection of digital content and services. XrML promotes the creation of open architectures for digital rights management. The developer has confirmed it will pass XrML to an international standards organization. Several standards organizations are discussing details of this governance role.	**DRM standards, coordinations, interests:** Major alliances—a number of large commercial entities support XrML (see XrML Web site). Other liaisons— OASIS, MEG-21 **Membership: NA** **See:** www.xrml.org **Remarks:** See entry for ODRL, above. XrML's specification has been submitted to both OASIS and MPEG-21. Discussion at www.xml.org/xml/zapthink/std263.html indicates differences between XrML and PRISM, the latter addressing a much simplified problem.
XTM Topic Maps *XML Topic Maps* presents ISO Topic Maps in XML. Handles "topics" and their occurrences and associations. Because not all e-text subjects are electronic artifacts, an address must be provided for such a subject, e.g. "George III." An electronic surrogate for the subject is constructed, which (being electronic) can have an address. This surrogate is a *topic*. Every topic acts as an e-link for some subject.	**DRM standards, coordinations, interests:** Major alliances Other liaisons— **Membership:** *TopicMaps.Org* is an independent consortium of parties developing the applicability of the topic map paradigm [ISO13250] to the World Wide Web by leveraging the XML family of specifications **See:** www.topicmaps.org/xtm/1.0/ **Remarks:** PRISM uses controlled vocabularies to similar end. See www.topicmaps.org/xtm/1.0/#desc-intro for easy-to-read discussion, including section 2.1, "A Gentle Introduction to Topic Maps."